ITRI 625

Pfleeger Chapter 6

Whitman & Mattord Chapters 6 & 7

Environment of use

- The biggest difference between a network and a stand-alone device is the environment in which each operates.

- Networks can be described by several typical characteristics:

  - Anonymity. A network removes most of the clues by which we recognize acquaintances.
  - Automation. In some networks most points involved might be machines with only minimal human supervision.
  - Distance. Networks connect endpoints with such speed that users typically cant tell whether a remote site is near or far.
  - Opaqueness. Users cannot distinguish where the node they are connected to is located. They cant even tell if they are communicating with the same host than the previous time.
  - Routing diversity. The same interaction might follow different paths each time it is invoked.

What makes a network vulnerable?

- Anonymity. An attack can be mounted without ever coming into contact with the system, its administrators, or users.
- Many points of attack – both targets and origins. An attack can come from any host to any host, therefore many points of vulnerability.
- Sharing. Access is afforded to more users and systems. Access controls for single systems may be inadequate in networks.
- Complexity of system. A network OS is more complex than an OS for a single computing system. This inherent complexity makes it extremely difficult, if not impossible, to secure.
- Unknown perimeter. A network's expandability also implies uncertainty about the network boundary.
- Unknown path. There are many paths from one host to another. Network users seldom have control over the routing of their messages.

Main types of attacks

- Reconnaissance. For example port scans, for intelligence, for social engineering, etc.
- Threats in transit: Eavesdropping and Wiretapping. These types of threats can occur across all transmission media.
- Impersonation. For example authentication foiled by guessing, nonexistent authentication, masquerade, etc.
- Message confidentiality threats. For example misdelivery (although uncommon), exposure, traffic flow analysis, etc.
- Message integrity threats. For example falsification of messages and noise.

Main types of attacks *cont.*

- Format failures. For example malformed packets, protocol failures and implementation flaws.
- Web site vulnerabilities. For example web site defacement, application code errors, etc.
- Denial of service. For example transmission failure, connection flooding, traffic redirection, etc.
- Threats in active or mobile code. For example cookies, scripts, etc.
- Complex attacks. For example script attacks and building blocks.

Network security controls

- Architecture. Planning can be the strongest control, especially when planning to build in security as one of the key constructs.
    - Segmentation. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow.
    - Redundancy. Allowing a function to be performed on more than one node, to avoid "putting all your eggs in one basket".
    - Single points of failure. Is there a single point in the network that if it were to fail, could deny access to all or a significant part of the network?
    - Mobile agents. Mobile code and hostile agents are potential methods of attack, but they can also be forces for good.

Network security controls *cont.*

- Encryption. Encryption is probably the most important and versatile tool for a network security expert.
  - Link encryption. Data are encrypted just before the system places them on the physical communications link.
  - End-to-end encryption. Provides security from one end of a transmission to the other.
  - SSH encryption. Provides an authenticated and encrypted path to the shell or operating system command interpreter.
  - SSL encryption. SSL interfaces between applications and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server.

Network security controls *cont.*

- Strong authentication. Authentication may be more difficult to achieve securely because of the possibility of eavesdropping and wiretapping.
  - One-time password. Good for one use only.
  - Challenge-response systems. A more sophisticated one-time password scheme. Uses a device that functions as an intermediary for authentication.
  - Digital distributed authentication. Developed due to the need to authenticate nonhuman entities in a computing system.
  - Kerberos. Used for authentication between intelligent processes, such as client-to-server tasks, or a user's workstation to other hosts (see p. 461). Supports authentication in distributed systems.

Network security controls *cont.*

- Wireless security. Being so exposed, it requires special measures to protect communication.
  - SSID. The service set identifier is the identification of an access point.
  - WEP. Meant to provide users privacy equivalent to that of a dedicated wire.
  - WPA and WPA2. Addresses the security deficiencies known in WEP.
  - Alarms and alerts. Devices that are placed inside protected networks to monitor what occurs inside the networks.
  - Honeypots. Computer systems open to attackers with the ideal of catching them.

Firewalls

- A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network. Its purpose is to keep "bad" things outside a protected environment.

- Types of firewalls include:

1. Packet filtering gateways. The simplest type of firewall that controls access to packets on the basis of packet address or specific transport protocol type.

2. Stateful inspection firewalls. An improvement through maintaining state information from one packet to another in the input stream.

Firewalls *cont.*

3. Application proxies. A firewall that simulates the proper effects of an application so that the application receives only requests to act properly.

4. Circuit gateway. A firewall that essentially allows one network to be an extension of another

5. Guards. A sophisticated firewall that decides what services to perform on the user's behalf in accordance with its available knowledge, such as whatever it can reliably know of the outside user's identity, previous interactions, and so forth.

6. Personal firewalls. An application program that runs on a workstation to block unwanted traffic, usually from the network. Complements the work of a conventional firewall.

See table 6.6 on page 468 for a summary.

Intrusion detection systems

- A device, typically another separate computer, that monitors activity to identify malicious or suspicious events.

- Types of IDSs:

  - Signature based. Performs simple pattern matching and reports situations that match a pattern corresponding to a known attack type.

  - Heuristic based. Build a model of acceptable behavior and flag exceptions to that model.

  - Network based. A standalone device attached to the network to monitor traffic throughout that network.

  - Host based. Runs on a single workstation or client or host, to protect that one host.

Goals for IDSs

- An IDS should be fast, simple, and accurate, while at the same time being complete.

- An IDS could use some or all of the following design approaches:
  - Filter on packet headers.
  - Filter on packet content.
  - Maintain connection state.
  - Use complex, multipacket signatures.
  - Use minimal number of signatures with maximum effect.
  - Filter in real time, online.
  - Hide its presence.
  - Use optimal sliding time window size to match signatures.

Security for e-mail

- Threats to e-mails include:
  - Message interception (confidentiality).
  - Message interception (blocked delivery).
  - Message interception and subsequent replay.
  - Message content modification.
  - Message origin modification.
  - Message content forgery by outsider.
  - Message origin forgery by outsider.
  - Message content forgery by recipient.
  - Message origin forgery by recipient.
  - Denial of message transmission.

Security for e-mail *cont.*

- The requirements for secure e-mail include:

1. Message confidentiality.
2. Message integrity.
3. Sender authenticity.
4. Nonrepudiation.

- Encryption can be used to address all the requirements identified above. Not only the message is encrypted, but all the header information as well. A message integrity check can also be incorporated to further ensure integrity.

- Key management is however the major problem with e-mail encryption.

Questions

- Any questions?